GUTRIDE SAFIER LLP
Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
Hayley Reynolds (State Bar No. 306427)
hayley@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, California 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Kali R. Backer (admitted pro hac vice)
kali@gutridesafier.com
4450 Arapahoe Ave., Suite 100
Boulder, Colorado 80303
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

Brandon Briskin, on behalf of himself and those similarly situated, Plaintiff, v. Shopify Inc.; Shopify (USA) Inc.; and Shopify Payments (USA), Inc., Defendants.	Case No. 4:21-cv-06269 Second Amended Class Action Complaint Jury Trial Demanded

Plaintiff Brandon Briskin brings this action on behalf of himself and all others similarly situated against Shopify Inc., Shopify (USA) Inc., and Shopify Payments (USA), Inc. (collectively, "Shopify"). Plaintiff's allegations against Shopify are based upon information and belief and upon investigation of Plaintiff's counsel, except for allegations specifically pertaining to Plaintiff, which are based upon Plaintiff's personal knowledge.

Introduction

1. Shopify is an e-commerce platform that enables merchants to easily sell products online. Many of Shopify's customers are merchants who operate websites and mobile applications, such as IABMFG. Shopify created software code to enable merchants to integrate Shopify's payment forms into their applications. To that end, Shopify provides comprehensive documentation to its merchant customers, describing how to integrate payment forms into their websites and applications using the Shopify code, including how to omit Shopify branding such that the form appears to the consumer to belong to the merchant's website.

2. In fact, despite the appearance to consumers that their payment information is being sent to the merchant, it is intercepted by Shopify. When a merchant integrates the Shopify software code into a website or mobile application, consumers who desire to pay for a product or service are presented with Shopify payment forms, which are created by Shopify. The payment forms require the consumer to provide a variety of sensitive information, such as:

- name
- address
- telephone number

- email address
- complete credit card information, including cvc

3. Shopify also collects and, by sharing the data with its payment processor, Stripe, Inc., indefinitely stores sensitive information about consumers using its payment form such as:

- The consumers' internet IP addresses;
- the brand and model of the consumer's computers or electronic devices;
- the identities of the consumer's browsers;
- the operating systems that the consumer's devices were using; and
- the item(s) purchased by the consumer from the merchants' websites.

4. Although consumers using merchants' websites and mobile applications reasonably expect that they are communicating directly with the merchant, Shopify's software code is designed to enable Shopify's computer network to intercept those communications and redirect them to Shopify's computer network. Shopify, however, designed its payment forms to omit all Shopify branding. Accordingly, the consumer has no idea that Shopify is involved in the transaction in any way, let alone that Shopify will be obtaining, transmitting, storing, and/or evaluating the consumer's sensitive communications and information.

5. The Shopify code also surreptitiously installs tracking cookies on consumers' computers and mobile devices, which enable Shopify to identify a particular consumer and track his or her activities across its entire merchant network, enabling Shopify to gather even more sensitive data about the consumer including, without limitation, (i) the number of declined cards that the consumer

has used with Shopify merchants; (ii) how long ago one of the consumer's cards was last declined; (iii) whether the consumer had ever disputed a previous Shopify charge; (iv) whether any previous early fraud warnings were associated with the consumer; (v) the percentage of transactions that were authorized for the consumer over time; and (vi) the cards and other payment methods associated with the consumer's IP address. Shopify accomplishes this, in part, by using the payment processing product provided by Stripe.

6. Shopify does not use consumers' private information simply for the purposes of processing the payments in question. Instead, using its own database as well as Stripe, Shopify indefinitely stores the information and correlates all payments from the consumer made across its entire platform. Although Shopify does not inform consumers of this, much of this private information is provided to other merchants, including those who do not use the Shopify platform. For example, on information and belief, once a consumer has submitted a payment for a purchase from IABMFG, any of Stripe's millions of other merchant customers will then be able to use Stripe's Radar product to access the consumer's private information pertaining to that payment, as well as any other payment that Shopify processed for that consumer, in a profile for that consumer.

7. Consumers using Shopify payment forms on merchant websites are not required to consent to any of Shopify's activities, and therefore are unaware that: (i) Shopify will intercept communications that consumers believe are being sent exclusively to merchants; (ii) its software code is causing their devices to connect to Shopify's computer servers; (iii) Shopify is accessing consumers' data by placing tracking cookies on their devices; (iv) its software code is rendering the payment forms that are displayed to consumers; (v) the sensitive information in

the payment forms will be sent to Shopify; (vi) sensitive information not expressly inputted by the consumer—such as IP address, operating system, geolocation data, and item(s) purchased—will also be collected from the consumer by Shopify; (vii) Shopify will indefinitely store that sensitive information using its own database and Stripe; (viii) consumers' private information will be used to create profiles of consumers, which could subsequently be communicated to other merchants on and off the Shopify network; (ix) Shopify will track consumers' behavior across over more than one million websites; and (x) consumers' sensitive information could be made available to millions of merchants who will accept payment—or who have already accepted payment—from those consumers.

Parties

8. Plaintiff Brandon Briskin is, and was at all relevant times, an individual and resident of California. Plaintiff currently resides in Madera, California.

9. Defendant Shopify Inc. is a Canadian company headquartered in Ottawa, Canada.

10. When merchants located in the United States sign up for Shopify's services, they enter into an agreement with Shopify Inc. for its online storefront, shopping cart, store management, marketing, and other services. Shopify Inc. focuses on direct-to-consumer brands. It directly contracts with thousands of California merchants, including IABMFG whose principal place of business is located in Sacramento, California. Some of Shopify Inc.'s largest merchant customers are California-based companies, including Kylie Cosmetics, Allbirds, Inc., and Fashion Nova.

11. Upon information and belief, in 2018, Shopify Inc. opened a physical

store located in Los Angeles, California that it uses to market its services to California merchants and to enhance its relationships with its existing California merchants. Shopify Inc.'s Chief Operating Officer at the time, Harvey Finkelstein, further explained "[w]ith Shopify LA we wanted to create a hub where business owners can find support, inspiration, and community."

12. A Shopify Inc. vice president at the time, Satish Kanwar, explained that "[i]t made sense for us to debut in the Los Angeles market as the region is one of our densest in customer base." As of 2018, Shopify Inc. had over 80,000 merchants located in California, with 10,000 located in the Los Angeles area alone. It also had over 400 merchants in the Los Angeles area who had over $1 million in gross merchandise volume (i.e. the total dollar value of orders facilitated through the Shopify platform). The gross merchandise volume is directly correlated with Shopify's revenues since for Shopify Payments transactions, fees are determined based in part on a percentage of the dollar amount processed plus a per transaction fee, where applicable. Through its Los Angeles store and its relationships with California merchants, Shopify Inc. has continuously and deliberately exploited the California market.

13. Upon information and belief, Shopify Inc. also partners with logistics firms to offer shipping services to its merchants to ship orders of 10 to 10,000 items from fulfillment centers located in the United States, including at least one in California. Merchants who use this service ship their goods to Shopify Inc.'s fulfillment centers, including the one in California, and Shopify Inc. stores and ships the goods for online orders, including to consumers located in California. Upon information and belief, through its fulfillment centers, Shopify Inc. ships thousands of packages to California.

14. Defendant Shopify (USA) Inc. is a Delaware company with its principal place of business in Ottawa, Canada. Shopify (USA) Inc. is registered to do business in California and had a domestic office in San Francisco, California. Shopify (USA), Inc. is a wholly owned subsidiary of Shopify Inc. A quarter of Shopify (USA), Inc.'s employees are located in California, and Shopify (USA), Inc. provides its services to thousands of California businesses. Shopify (USA), Inc. further collects and processes California consumers' personal information from Shopify's platform. Shopify Inc. designates Shopify (USA), Inc. as a subprocessor of user data.

15. Defendant Shopify Payments (USA) Inc. is a Delaware company with its principal place of business in Wilmington, Delaware. Shopify Payments (USA), Inc. is a wholly owned subsidiary of Shopify Inc. Shopify Inc. offers its merchants a separate and additional feature that enables Shopify merchants to accept and process online credit and debit payments. In order to obtain these services, a Shopify merchant must enter into a separate contract with Shopify Payments (USA), Inc. Under that contract, Shopify Payments (USA), Inc. and Stripe provide the payment software to Shopify merchants. The contract discusses how Shopify Payments (USA), Inc. and Stripe will collect, use, process and disclose users' personal information. It further provides that "[Stripe] and MaxMind, a fraud detection service, each independently serve as 'data controllers' with regards to any personal data that they may processes under this Agreement and that we are not responsible for how they process such data." The contract further allows Shopify Payments (USA), Inc. to charge fees based for the payment processing servings. Upon information and belief, Shopify Payments (USA), Inc. contracts with thousands of California merchants.

16. Since at least 2014, Shopify Inc. and Shopify Payments (USA), Inc. have relied exclusively on Stripe to conduct the payment processing services that they offer Shopify merchants. To accomplish this, Shopify Payments (USA), Inc. contracted with Stripe, a company with its principal place of business in California, to provide payment processing services. Shopify Inc. is a third party beneficiary under that agreement.

17. Upon information and belief, through that contact, Shopify Payments (USA), Inc. shares with Stripe thousands, if not millions, of California consumers' private information and transaction information and has enabled Stripe, Inc. to develop user profiles on those California consumers. Shopify Inc.'s relationship with Stripe has become a cornerstone of its business since it enables its merchants do business online. Shopify Inc. recently deepened its ties with Stripe, Inc. by investing over $350 million in Stripe.

18. Shopify Inc., Shopify (USA) Inc., and Shopify Payments (USA), Inc. are referred to collectively herein as "Shopify."

Jurisdiction and Venue

19. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. Section 1332(d)(2)(A) because: (i) there are 100 or more class members, and (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs.

20. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

21. The injuries, damages and/or harm upon which this action is based occurred or arose out of activities engaged in by Shopify within, affecting, and emanating from the State of California. Shopify regularly conducts and/or solicits

business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products provided to persons in the State of California. Shopify has engaged, and continues to engage, in substantial and continuous business practices in the State of California.

22. Venue is proper in this District pursuant to 28 U.S.C. Section 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in the state of California, including within this District.

23. Plaintiff accordingly alleges that jurisdiction and venue are proper in this Court.

Substantive Allegations

A. Shopify Surreptitiously Intercepts Consumers' Communications and Collects their Private Information When They Make Online Payments to Merchants.

24. Shopify is an e-commerce platform that enables merchants to sell products online. In June 2019, Shopify reported that it had more than 1,000,000 businesses in approximately 175 countries using its platform, with total gross merchandise volume exceeding $41 billion for calendar year 2018.[1] Using Shopify's website, merchants provide Shopify with their product offerings, prices, shipping options and other business preferences. Shopify hosts some of its merchants' websites and creates all of the code necessary to implement the product catalog and to accept payment. In addition, merchants who already own websites can elect to embed certain Shopify assets, such as payment forms, into their pre-existing websites. Regardless of the implementation, Shopify handles the

[1] Shopify Announces Fourth-Quarter and Full Year 2018 Financial Results, Businesswire.com, available at: https://www.businesswire.com/news/home/20190212005234/en/ (last accessed August 2, 2021).

collection and validation of the consumer's payment information, as well as processing the payment, through its relationships with third parties, such as Stripe.

25. To display payment forms to consumers, Shopify sends executable javascript code to consumers' computers or mobile devices, which then execute the code. Upon execution, the code loads and displays the payment forms to consumers.

26. Shopify does not disclose to consumers its role in the transaction, let alone that Shopify is sending code to consumers' devices to display the payment forms. To the consumer, the website and payment forms appear to be generated by the merchant itself. Thus, a consumer never knows that they have shared their sensitive information, including sensitive financial information, to Shopify, nor does the consumer consent to such actions.

27. For example, consumers who order apparel or accessories on the IABMFG website are presented with a cart page before proceeding to the checkout page. The bottom of the cart page features a number of icons for various forms of payment, including Visa, Mastercard and American Express. The Shopify icon is presented alongside the credit card icons, making it appear to consumers that Shopify is optional or a type of payment method the consumer could choose akin to a credit card even though it is not.

28. Consumers who proceed with purchasing goods on the IABMFG website are presented with the following payment form where there is no mention of Shopify:

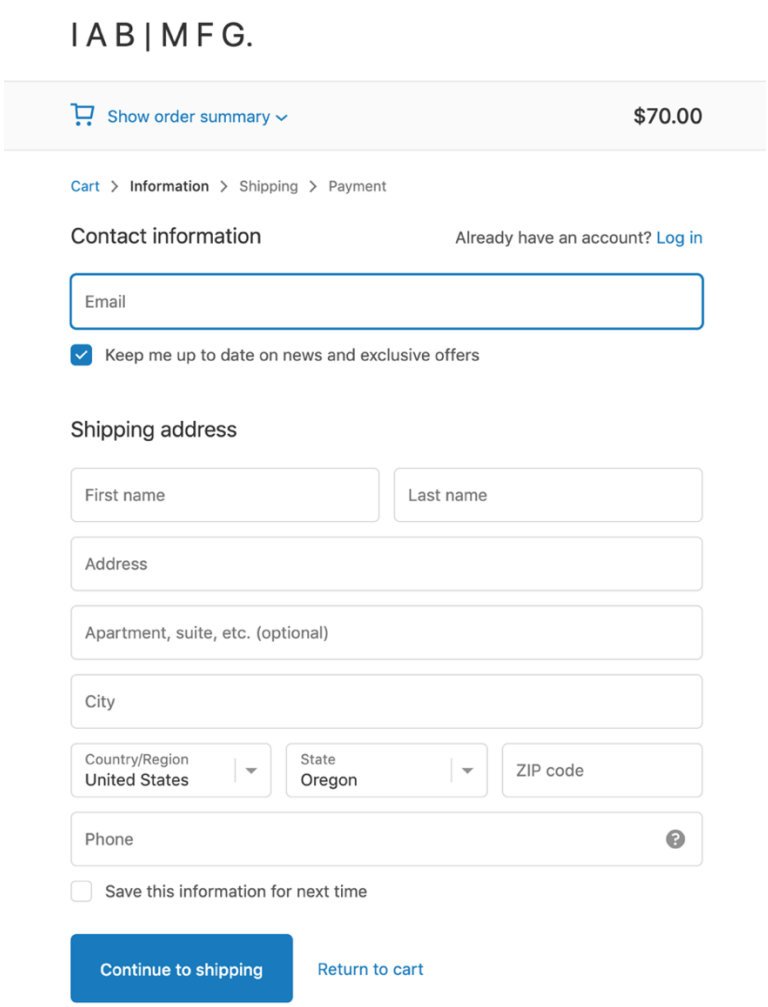

Figure 1: IABMFG Checkout Page

29. All of the input elements in the form (i.e., those corresponding to "Email," "First name," "Last name," "Address," "Apartment, suite, etc.," "City," "Country/Region," "State," "ZIP code," and "Phone") are generated by Shopify.[2] To the user, however, it appears that the form and input elements are generated and provided by IABMFG. Shopify does not cause its involvement in the transaction to be displayed to the consumer alongside the payment form.

[2] This is confirmed by the fact that the input elements are located in a tag having the class "edit_checkout"—a class that Shopify uses throughout its network of merchant websites.

30. Only a person with technical knowledge and special software tools could determine that the payment forms are generated by Shopify. As shown by the following screenshot from such a tool, the IABMFG checkout page above required the user's browser to load at least eight separate files—including four executable javascript files—from Shopify's computer network:

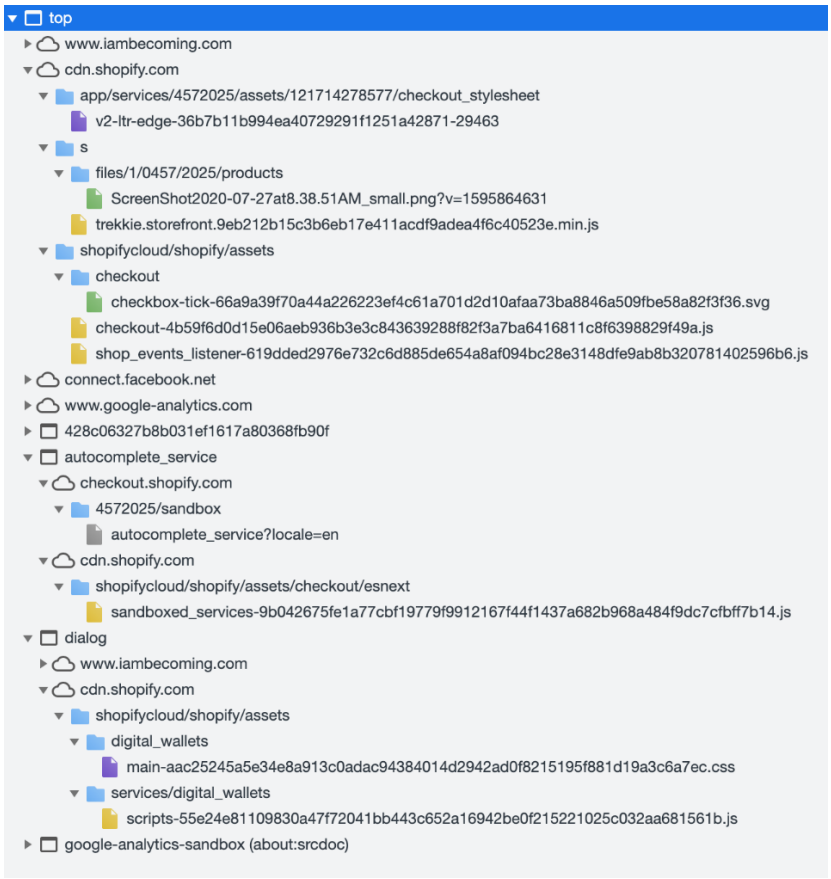

Figure 2: Assets loaded from Shopify during rendering of IABMFG checkout page

31. After submitting the shipping information form on the IABMFG website, the user is presented with a payment form where again there is no mention of Shopify:

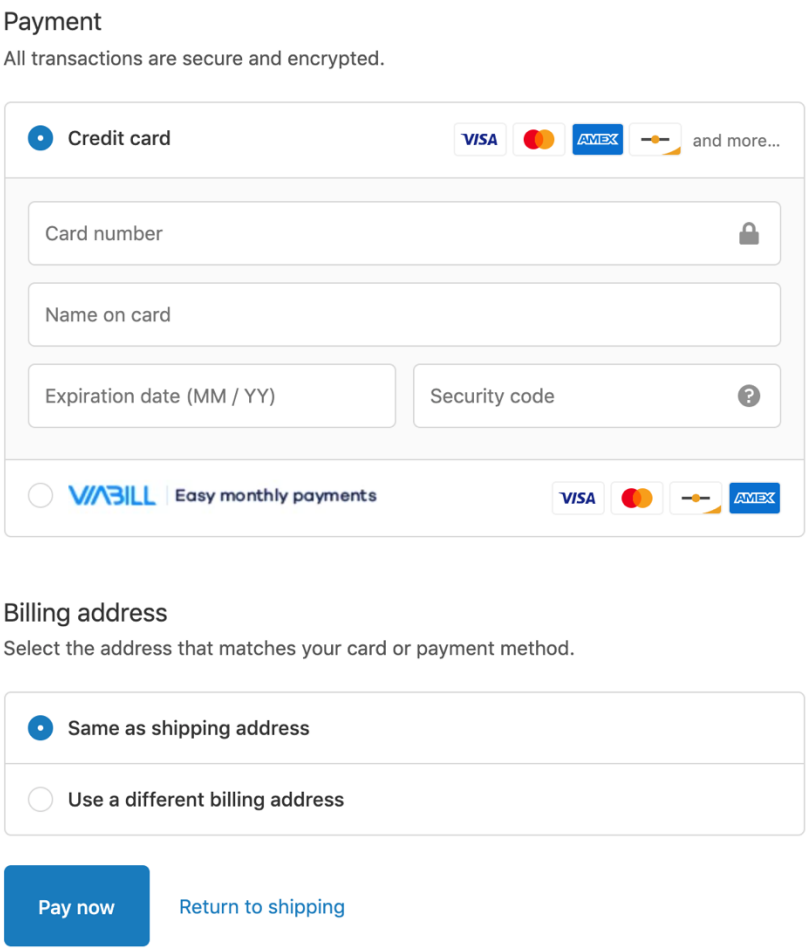

Figure 3: IABMFG Payment Form

32. Once again, the payment form—including the input elements—is generated by Shopify and sent to the user's browser. To the user, however, it appears that the payment form is being generated by the IABMFG website. As is true of the shipping form, Shopify does not disclose its involvement in the transaction to the consumer.

33. When the user clicks the "Pay now" button, the Shopify-produced javascript code is executed on the user's computer, causing the payment details to be collected from the form, and then sent directly to Shopify's servers, at https://deposit.us.shopifycs.com/sessions. For example, the payload sent to that

address in a test transaction conducted on April 12, 2021, as seen through a special software tool, was as follows:

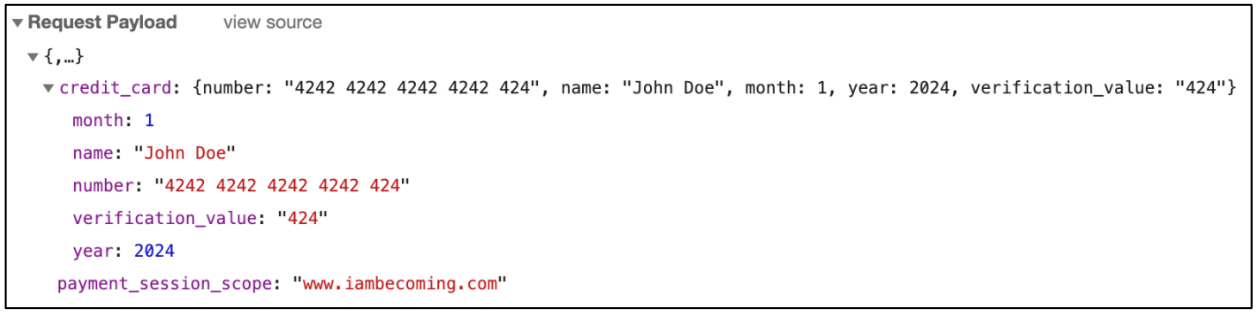

Figure 4: Request Payload to Shopify

34. As the figure above displays, the data sent directly to Shopify includes the user's name and sensitive payment information. This payload request, however, is just one of many requests that Shopify causes the user's browser to make to Shopify. Dozens of urls were also called by the user's browser upon clicking the "Pay now" button during the April 12 test transaction. None of these url calls are visible to the consumer.

35. When a consumer completes and submits the shipping and payment forms, it appears to the consumer that the information in the forms will be sent directly to the merchant. However, Shopify's software code, which has been installed on the user's computer without his or her consent, ensures that consumers' communications—including the private information in the forms—are intercepted and rerouted to Shopify's computer servers, including the servers that receive the requests listed above.

36. After the consumer has completed a purchase transaction, Shopify sends the user an order confirmation email. The email does not mention Shopify, let alone disclose to the consumer that Shopify has obtained his or her sensitive information and communications and/or that it will store the consumer's sensitive

information and communications using its database and/or Stripe. Instead, it appears that it was sent by the merchant. The "From" email address is identical to the merchant's email.

37. The receipt email that Shopify sends to consumers contains a button entitled "View your order." Consumers who click the button are taken to the merchant's website and are shown a webpage that, although hosted and/or created by Shopify, does not mention Shopify or disclose its involvement. Rather, to the consumer, the page appears to have been created and hosted by the merchant.

38. Shopify's involvement with the consumer's private information does not end when the transaction is completed. To the contrary, Shopify's involvement has only begun. Now that Shopify has the consumer's information, Shopify will track the consumer's behavior across its vast merchant network. To achieve this, Shopify installs a tracking cookie on the user's browser. This cookie may be installed when the user visits the payment page, or any other page of the merchant's website.

39. For example, merely viewing a single item on the IABMFG website (the IABMFG Flex High Waisted Capri Pants, at https://www.iambecoming.com/collections/iab-flex-high-waisted-capri) caused at least six Shopify tracking cookies to be installed on the browser:

- _shopify_sa_p
- _shopify_sa_t
- _shopify_s
- _shopify_y
- _shopify_fs
- _shopify_country

40. Although the contents of Shopify cookies are encrypted, such that one cannot view their contents without the decryption key, it is known that these cookies are used to track consumers, their devices, and their behavior. The cookie "_shopify_y," for example, contains a unique code that uniquely identifies the consumer's device, so that Shopify can track the consumer's behavior across its vast merchant network. Further, it is known that Shopify collects at least the following information about customers of merchants such as IABMFG:

- name;
- email address;
- company;
- shipping address;
- billing address;
- phone number;
- amount spent;
- IP address;
- user agent (i.e., the user's browser); and
- geolocation data.

41. This information is stored either by Shopify and/or by Stripe after the information is provided to it by Shopify. Shopify and/or Stripe make ***all*** of this information available to its merchants who are involved in transactions with the consumer in question. To retrieve the information, a merchant can click a button entitled "View customer data" in the Shopify user interface, and Shopify will email the data corresponding to the transactions with the merchant and consumer.

B. Shopify Discloses and Sells Consumers' Sensitive Information to Merchants, and Uses it to Assess Transaction Risk.

42. Because over one million websites and other merchants use Shopify to sell their products, Shopify has amassed an incredible amount of sensitive data regarding consumers. Shopify leverages this data to assess the risk associated with particular consumers and their transactions. This information is used to assign risk scores to consumers' transactions, which can affect consumers' ability to complete future transactions with merchants on and off the Shopify network. Payment transactions with unacceptable indicators can be blocked or reversed.

43. In addition, Shopify makes information in the user profiles available to its merchant customers. For example, Shopify merchants can view a variety of information regarding the consumer transactions:

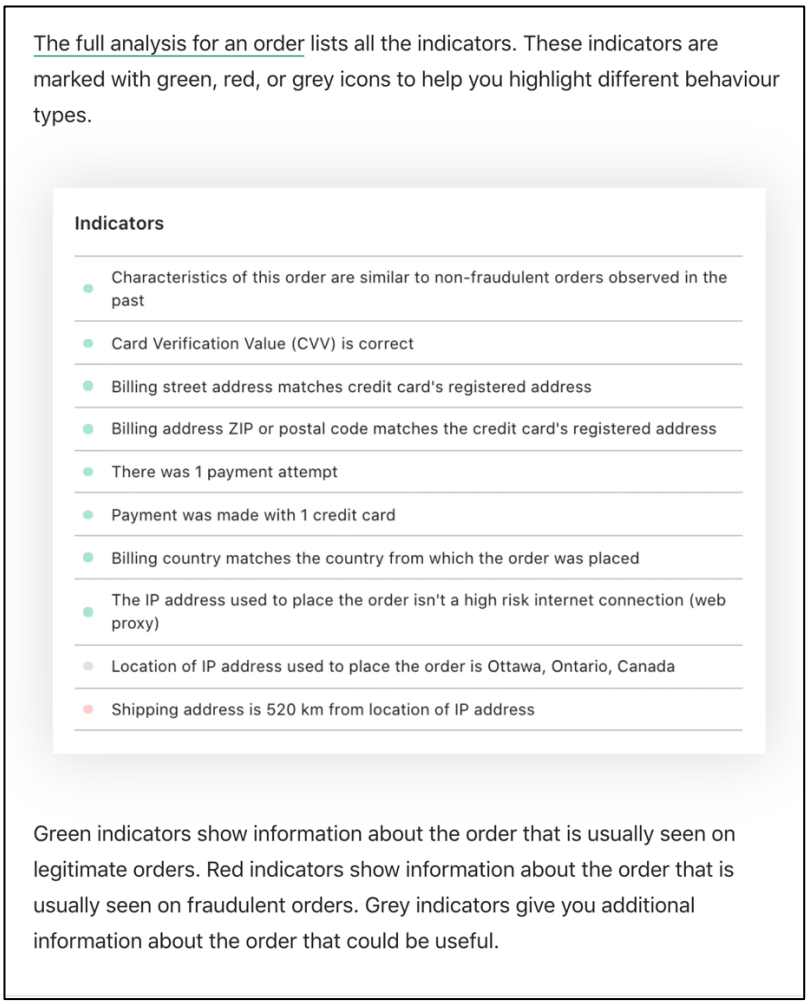

Figure 5: Shopify Analysis Indicators

44. At no time does Shopify obtain consumers' consent to enable it to collect and use their sensitive payment information.

45. In fact, Shopify enables its merchant customers to set filters that can preemptively block orders based on the information that Shopify collects on consumers. Through the filters, Shopify's merchant customers can set rules that can ban IP addresses, prevent certain customers from placing orders, and automatically cancel orders that have "high" risk scores, among other things. When a filter preemptively cancels an order, the consumer has no idea. Rather, from the consumer's perspective, the order processes normally. But, in reality, the

order is "accepted" and then immediately canceled. Consumers will only see that their credit card was declined, which can negatively impact the "score" that Shopify assigns to the consumer and lead to future cancellations.

46. In addition to compiling risk profiles for each consumer and/or transaction, Shopify also shares the information that its collects on consumers with third-parties, who, in turn, use the consumers' data for their own purposes and share it with others. For example, Shopify partners with Stripe, Inc. to handle payment processing. When a consumer fills out a payment form, Shopify collects information regarding the transaction and consumer. Shopify then shares that information with Stripe, which enables Stripe to process the payment. Stripe creates "risk insights" profiles for consumers, which include sensitive information, such as (i) the number of declined cards previously associated with an email address, (ii) the time since the first card decline occurred, (iii) the IP address, and (iv) the credit card number. Upon information and belief, Stripe uses the data that Shopify shares with Stripe to process payments to build out its own risk profiles on consumers, which it then markets and disseminates to its own customers.

47. Shopify also shares consumers' information with MaxMind which MaxMind uses to create consumer risk profiles. When a user purchases an item through one of Shopify's merchant customers, Shopify provides MaxMind with the consumers' personal information and data regarding the transaction. MaxMind uses that information to assign a risk score to the consumer and transaction, which Shopify, in turn, shares with its merchant customers to evaluate the transaction and—on information and belief—future transactions. MaxMind also markets and disseminates the consumer risk profiles to its own customers.

48. Because Shopify conceals its involvement with consumer transactions, consumers are unaware that Shopify shares their sensitive information with third parties and are deprived of any ability to opt out of the dissemination of their data from Shopify and the third-parties that are also receiving their sensitive data.

49. Shopify's collection, storage and dissemination of users' sensitive information opens consumers to the possibility of identity theft, credit card theft, and fraud, by storing their information, without their knowledge or consent, creating a new venue that is open to vulnerabilities, such as hackers and phishing scams. However, consumers who do not even know that their information is collected and stored by Shopify and/or Shopify's payment processor Stripe. Nor do consumers know that their information is shared by Shopify with other third parties. Thus consumers will not know to be weary of scams, and are deprived of the knowledge necessary to protect their data.

50. The potential for identity theft, credit card theft and fraud of data secretly collected and stored by Shopify is more than a mere possibility. From 2019-2020, certain Shopify staff members took advantage of the consumer data Shopify unlawfully collected and stored. Shopify announced in September 2020 that it became aware of an incident in which data from about 200 merchants was stolen.[3] These staff members acquired information regarding consumer transaction on Shopify's platform. The data included consumer names, e-mails, addresses, and order details, including products, services purchased, payment methods, and the last four digits of their credit cards.[4] The staff members later sold the data to others on the black market. It has been estimated that the data

[3] *See* https://community.shopify.com/c/Shopify-Discussion/Incident-Update/td-p/888971 (last accessed August 2, 2021).

[4] *See* https://www.documentcloud.org/documents/20580321-us-grand-jury-indictment-tassilo-heinrich (last accessed August 2, 2021).

breach involved the data of about 272,000 individuals. The consumer data that is now in the hands of criminals was data that Shopify was never authorized to collect at the outset. Because Shopify concealed its involvement with the transactions, Shopify deprived consumers of the right to opt out of its collection of their private information and, in doing so, has exposed consumers to the risk, and for some consumers, the reality of identity theft, credit card theft and fraud.

C. Shopify Does Not Inform Consumers About Its Activities.

51. Shopify makes no effort to inform consumers regarding ***any*** of its activities with respect to its interception and collection of consumer information using merchant websites. Specifically, it does not inform consumers that: (i) Shopify will intercept communications that consumers believe are being sent exclusively to merchants; (ii) its software code is causing their devices to connect to Shopify's computer servers; (iii) Shopify is placing tracking cookies on consumers' computers; (iv) its software code is rendering the payment forms that are displayed to consumers; (v) the sensitive information in the payment forms will be sent to Shopify; (vi) sensitive information not expressly input by the consumer—such as IP address, operating system, geolocation data, and item(s) purchased—will also be collected from the consumer by Shopify; (vii) Shopify and/or its payment processor Stripe will indefinitely store that sensitive information; (viii) Shopify will use consumers' information to assign risk scores to consumers and/or transactions, which could subsequently be communicated to other merchants and used to deny consumers' future payment attempts; (ix) Shopify will track consumers' behavior across over one million websites; (x) Shopify will make consumers' sensitive information available to any of its millions of customers who will accept payment—or who have already accepted

payment—from those consumers; and (xi) Shopify will share consumer data with third-parties, such as Stripe, Inc. and MaxMind, Inc. Nor does Shopify obtain consent from consumers before taking any of the aforementioned activities.

52. Shopify deliberately chose to hide its involvement from consumers. Shopify did so to increase its profits, because it (i) understands that consumers value the privacy of their communications and do not wish those communications to be intercepted; (ii) understands that consumers do not wish for their activities to be tracked across a vast network of third party merchants; and (iii) wants to maximize the ability of its merchant customers to "white-label" payment forms, to make it appear to consumers that the merchants have the sophistication to handle payments themselves and without extensive third party involvement.

53. Although Shopify provides a default template for merchant websites that includes, in the footer, a "powered with Shopify" link leading to Shopify's homepage, Shopify does not require merchants to use that template, or the link. Indeed, Shopify provides instructions—including a dedicated video—to merchants regarding how to remove the link. (See https://help.shopify.com/en/manual/online-store/themes/os/customize/remove-powered-by-shopify-message (last accessed August 9, 2021).) As Shopify knows, the vast majority—if not all—of its large merchants delete the link.

54. On information and belief, Shopify does not review its customers' websites or mobile applications to determine whether its customers have disclosed to consumers any of Shopify's activities with respect to their personal information. On information and belief, Shopify does not review its customers' websites or mobile applications to determine whether the merchants require customers to obtain consent from consumers to allow Shopify to take any

activities with respect to their personal information.

55. Consumers visiting Shopify merchants' webpages are not required to view (through a link or otherwise), let alone agree to, Shopify's Terms of Service or Privacy Policy. Plaintiff has never agreed to any such policy.

56. As described above, the information that Shopify obtains from consumers who purchase products from merchants utilizing the Shopify payment forms includes consumers' telephone numbers. Shopify maintains a database of these consumer telephone numbers on its computers. Shopify then transmits, or causes to be transmitted by a third party, marketing text messages to selected telephone numbers from Shopify's database. For example, Shopify sends "abandoned cart" text messages to consumers that add items to their cart but do not complete the checkout process. The telephone numbers messaged by Shopify are assigned to cellular telephone service for which Plaintiff and Class members incur charges for incoming messages.

D. Plaintiff's Experience

57. Plaintiff purchased fitness apparel for his wife from IABMFG on or about June 14, 2019. To do so, he used his iPhone's Safari browser to establish a secure, encrypted connection to IABMFG at https://www.iambecoming.com.

58. After adding products to his virtual shopping cart, Plaintiff was presented with a checkout screen substantially similar to the screen shown at Figure 1, *supra.* Plaintiff believed that all aspects of the checkout screen were being generated by IABMFG, and sent over his browser's encrypted connection with IABMFG.

59. Plaintiff was required to provide his private information in order to complete the checkout process, including information such as his full name,

delivery address, billing address, phone number, and credit card number, expiration date, and CVV code. Plaintiff provided this information, and then clicked on the "Pay now" button to submit it. Plaintiff did not provide consent to Shopify to send him text messages. Plaintiff did not provide consent for Shopify to obtain, use, store, or share his sensitive information. When Plaintiff clicked the "Pay now" button, he believed that his information would be sent directly to IABMFG, through the secure, encrypted connection that his smartphone browser had established with IABMFG.

60. Although Plaintiff was not aware of it, the IABMFG checkout page he visited contained a link to the Shopify software code, which caused his smartphone browser to load and execute the code. Although it was not disclosed to Plaintiff, this code (i) enabled Shopify to intercept communications—including those with his private information—that he reasonably believed would be sent exclusively to IABMFG; (ii) enabled Shopify to install and/or confirm the installation of a tracking cookie, containing a unique tracking code, on his smartphone; (iii) caused his phone browser to establish a connection with Shopify's computer network; and (iv) generated the payment form input elements requiring Plaintiff to enter his private information. When Plaintiff submitted the form containing his private information to complete the checkout process, his private information was sent to Shopify's computer network, where it was stored, analyzed, and/or processed. Shopify also transmitted his information to its payment processor, Stripe, where it was stored, analyzed, and/or processed. Plaintiff was never informed of any of these facts. Indeed, Plaintiff did not know that Shopify was involved in the transaction at all, because it was never disclosed

to him. Nor did Plaintiff ever consent to Shopify's involvement or activities described herein.

61. Nearly every page on the IABMFG website—including the homepage or "index" page, as well as the pages corresponding to the IABMFG products for sale—contains a link to the company's "Privacy Policy," which leads to the url https://www.iambecoming.com/pages/legal. That privacy policy does not mention Shopify. Further, the privacy policy purports to provide a list of all the cookies that IABMFG uses, but the policy omits the cookies that Shopify uses when consumers transact with IABMFG. At some point—which, on information and belief, occurred after Plaintiff's transactions with IABMFG—the company modified its website such that when a user begins to the checkout process, the url for the "Privacy Policy" link surreptitiously changes to https://www.iambecoming.com/4572025/policies/privacy-policy.html. That page does refer to Shopify's involvement in transactions. However, consumers are not prompted to click the link or read the page, let alone agree to any terms on the page. Plaintiff never saw nor agreed to any privacy disclosures on the IABMFG website.

62. The private information that Shopify obtained from Plaintiff has been used to assign a score to his subsequent transactions other merchants that use the Shopify network and/or Stripe payment processing product. On information and belief, with Shopify's knowledge, Stripe has offered to make and/or actually made Plaintiff's private information available to any of Stripe's merchant customers who process payments made by Plaintiff. Shopify has shared Plaintiff's private information with third parties, such as Stripe, Inc., and MaxMind, Inc.

Shopify also used the private information collected from Plaintiff to send him unsolicited marketing emails and text messages about IABMFG's products.

63. Had Plaintiff known that Shopify would install a tracking cookie on his smartphone browser, for the purpose of tracking him across potentially hundreds of thousands, if not millions, of websites, Plaintiff would not have purchased products from IABMFG.

64. Had Plaintiff known that Shopify would collect, store, analyze, and/or transfer his private information to increase its own profits, Plaintiff would not have purchased products from IABMFG.

65. Had Plaintiff known that his private information would be made available to potentially millions of merchants with whom he may engage in a subsequent financial transaction, Plaintiff would not have purchased products from IABMFG.

66. Had Plaintiff known that his private information would be used to create a risk profile on him based on his subsequent transactions, Plaintiff would not have purchased products from IABMFG.

Class Allegations

67. In addition to his individual claims, Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

68. Plaintiff brings this class action lawsuit on behalf of a proposed class of similarly situated persons, pursuant to Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure, defined as follows:

> The Class: All natural persons who, between August 13, 2017 and the present, submitted payment information via Shopify's software while located in California.

69. This action has been brought and may properly be maintained as a class

action against Shopify because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

70. Numerosity: Plaintiff does not know the exact size of the Class, but he estimates that the Class is composed of more than 5,000 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

71. Common Questions Predominate: This action involves common questions of law and fact to the potential Class because each class member's claim derives from the same unlawful practices of Shopify. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class include, but are not limited to, whether Shopify has violated Sections 631 and 635 of the California Invasion of Privacy Act; whether Shopify invaded the Class members' privacy rights in violation of the California Constitution; whether Shopify violated the California Computer Data Access and Fraud Act; whether Shopify violated California's Unfair Competition Law; and whether the Class members are entitled to actual damages, statutory damages, and/or equitable relief for these violations.

72. Typicality: Plaintiff's claims are typical of the claims of other Class members because, among other things, all such claims arise out of the same unlawful course of conduct in which Shopify engaged. Plaintiff and those similarly situated used Shopify payment forms and had their electronic communications intercepted and disclosed to Shopify through the use of Shopify's wiretaps.

73. Adequacy of Representation: Plaintiff will fairly and adequately protect the interests of all class members because it is in his best interests to prosecute the claims alleged herein to obtain full compensation due to him for the unfair and illegal conduct of which he complains. Plaintiff also has no interests that are in conflict with, or antagonistic to, the interests of Class members. Plaintiff has retained highly competent and experienced class action attorneys to represent his interests and those of the Class. By prevailing on his own claims, Plaintiff will establish Shopify's liability to all Class members. Plaintiff and his counsel have the necessary financial resources to adequately and vigorously litigate this class action, and Plaintiff and counsel are aware of their fiduciary responsibilities to the class members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for class members.

74. Superiority: There is no plain, speedy, or adequate remedy other than by maintenance of this class action. The prosecution of individual remedies by members of the class will tend to establish inconsistent standards of conduct for Shopify and result in the impairment of class members' rights and the disposition of their interests through actions to which they were not parties. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. Furthermore, as the damages suffered by each individual member of the class may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action.

75. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

First Cause of Action

Violation of the California Invasion of Privacy Act, California Penal Code § 631 (On Behalf of Plaintiff and the Class)

76. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

77. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to 638 ("CIPA"), includes the following statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

78. To establish liability under section 631(a), a plaintiff need only establish that a defendant, "by means of any machine, instrument, contrivance, or in any other manner," did any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any

> message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

(Cal. Penal Code § 631(a).)

79. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google* Inc., 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

80. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA (and even if they do not, Shopify's deliberate and purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner"): (i) Shopify's software code modules that are designed to intercept, collect, transmit, and track consumers' private information; (ii) the Shopify computer servers, including the software code modules installed on those servers used to intercept, receive, transmit, read, track, analyze, and sell such private information; and (iii) the plan Shopify carried out to intercept, collect, transmit, read, track, analyze, and sell the Class members'

private information, even though they had not consented (collectively, (i), (ii), and (iii) are referred to hereinafter as the "Shopify Instruments").

81. The private information that was intercepted, collected, transmitted, received, tracked, and analyzed by the Shopify Instruments included at least the following information regarding each consumer:

- full name;
- home and/or delivery address;
- billing address;
- telephone number;
- email address;
- credit and/or debit card number, expiration date, and CVV number;
- internet IP addresses;
- the item(s) purchased from the merchant;
- the brand and model of the consumer's computers or electronic devices;
- the identities of the consumer's browsers;
- the operating systems that the consumer's devices were using;
- the unique tracking codes, which enable Shopify to identify a particular consumer and track his or her activities across its entire merchant network, enabling Shopify, through its use of the Stripe platform, to gather even more sensitive data about the consumer including, without limitation, (i) the number of declined cards that the consumer has used with Shopify merchants; (ii) how long ago one of the consumer's cards was last declined; (iii) whether the consumer had ever disputed a previous Shopify charge; (iv) whether any previous early fraud warnings were associated with the consumer; (v) the percentage of transactions that were authorized

for the consumer over time; and (vi) the cards and other payment methods associated with the consumer's IP address.

(collectively, the information listed in the bullet points above shall be referred to as "Private Information.")

82. Specifically, the code caused the Private Information that the consumer intended to send to the merchant to instead be intercepted by the Shopify Instruments while in transit to the merchant. The merchant does not receive the Private Information and share it with Shopify, but instead it goes directly to Shopify.

83. Shopify never had authorization or consent from the consumers to intercept and collect the Private Information.

84. By enabling the Shopify Instruments to intercept, collect, transmit, receive, track, and analyze consumers' Private Information without their consent, and by communicating and selling that Private Information to Shopify merchants, Shopify violated Section 631(a) of the Privacy Act. In particular, Shopify:

- intentionally tapped, electrically or otherwise, the lines and/or instruments of internet communication being used by Class members to access merchant websites;
- intentionally made unauthorized connections, electrically or otherwise, with the lines and/or instruments of internet communication being used by Class members to access merchant websites;
- willfully, and without the consent of Class members, read and learned the contents and/or meaning of their messages and communications containing private information, while the same was in transit or passing

over lines of internet communication, or was being sent from and received at locations in California;

- used Class members' Private Information to increase Shopify's profits;
- communicated and/or sold Class members' Private Information to Shopify's merchant customers;
- communicated and/or sold Class members' Private Information to third parties, such as Stripe and MaxMind; and
- aided, agreed with, and conspired with other persons (including, without limitation, IABMFG, Stripe, and MaxMind) to unlawfully do, permit, and cause to be done the above-listed activities.

85. The Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of their right to privacy; (ii) loss of value in their Private Information; and (iii) the price premium they were unknowingly charged by IABMFG to compensate for Shopify's fees, since they would not have entered into such financial transactions had they known their Private Information would be intercepted, collected, shared and used.

86. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing.

87. Unless enjoined, Shopify will continue to commit the illegal acts alleged here. The Class Members continue to be at risk because they frequently use the internet to search for information about products and services. They continue to desire to use the internet for that purpose, including for the purpose of shopping for various products and services. Shopify has intentionally designed its payment forms to omit reference to Shopify, and to appear as though Shopify is not involved in the transaction. Accordingly, the Class Members have no practical

way to know if their website communications will be monitored or recorded by Shopify and/or if Shopify will collect further Private Information from them. Further, Shopify has already collected their Private Information, and is currently sharing, and will continue sharing, that information with its other merchant customers and third parties, unless and until enjoined by this Court.

88. The Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

Second Cause of Action

Violation of the California Invasion of Privacy Act,
California Penal Code § 635
(On Behalf of Plaintiff and the Class)

89. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

90. California Penal Code § 635 provides as follows:

> Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones or between a cellular radio telephone and a landline telephone in violation of Section 632.5, or communications between cordless telephones or between a cordless telephone and a landline telephone in violation of Section 632.6 , shall be punished by a fine not exceeding two thousand five hundred dollars.

91. Shopify intentionally manufactured, assembled, sold, offered for sale, advertised for sale, possessed, transported, imported, and/or furnished one or more wiretap devices (i.e., the Shopify Instruments, including the software code

modules therein) primarily or exclusively designed or intended for eavesdropping upon the communication of another.

92. In particular, the Shopify Instruments contain software code modules that are primarily or exclusively designed to intercept, collect, transmit, receive, and track communications that Class members reasonably (but erroneously) believed would be sent directly and exclusively to the merchant. Further, although the Class members intended to provide only information necessary for the purchase of products and services, and to provide that information directly and exclusively to the merchant, the software code modules of the Shopify Instruments were designed to (and in fact did) intercept, collect, transmit, receive, track, analyze, and sell the Private Information of the Class members.

93. The Class members did not consent to any of Shopify's actions in implementing its wiretaps.

94. The Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of their right to privacy; (ii) loss of value in their Private Information; and (iii) the price premium they were unknowingly charged by IABMFG to compensate for Shopify's fees, since they would not have entered into such financial transactions had they known their Private Information would be intercepted, collected, shared and used.

95. The violation of section 635 constitutes an invasion of privacy sufficient to confer Article III standing.

96. Unless enjoined, Shopify will continue to commit the illegal acts alleged here. The Class members continue to be at risk because they frequently use the internet to search for information about products and services. They continue to desire to use the internet for that purpose, including for the purpose of

shopping for various products and services. Defendant Shopify has intentionally designed Shopify's payment forms to omit reference to Shopify, and to appear as though Shopify is not involved in the transaction. Accordingly, the Class Members have no practical way to know if their website communications will be monitored or recorded by Shopify and/or if Shopify will collect further Private Information from them. Further, Shopify has already collected their Private Information, and is currently sharing, and will continue sharing, that information with its other merchant customers and/or third parties, unless and until enjoined by this Court.

97. The Class members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

Third Cause of Action

Invasion of Privacy Under California's Constitution (On Behalf of Plaintiff and the Class)

98. Plaintiff realleges and incorporates the paragraphs of this Class Action Complaint as if set forth herein.

99. California's constitution creates a right to privacy, and further creates a right of action against private entities such as Shopify.

100. The principal purpose of this constitutional right is to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Shopify.

101. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (i) a legally protected privacy interest; (ii) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (iii) conduct by the defendant constituting a serious invasion of privacy.

102. Shopify has intruded upon the following legally protected privacy interests of the Class members: (i) the California Wiretap Act as alleged above; (ii) the California Constitution, which guarantees Californians the right to privacy; and (iii) a Fourth Amendment right to privacy.

103. The Class members had a reasonable expectation of privacy. They directed their electronic devices to access merchant websites, such as IABMFG, and to form an encrypted connection with those websites, such as https://www.iambecoming.com. When they were presented with the payment form on merchants' websites, such as IABMFG's, they reasonably expected that only some of their Private Information would be sent, in encrypted form, to the merchant, such as IABMFG. They reasonably expected that no third party, such as Shopify, would intercept and obtain the Private Information they submitted using the forms. They further reasonably expected that no third party, such as Shopify, would obtain Private Information about them that was not included on the form, such as their IP addresses, device identities, and operating systems. The Class members further reasonably expected that no one would store and assemble their information, make profiles about them, and then make those profiles and Private Information available to other merchants—which is what happens when consumers do business with Shopify merchants. The Class members further reasonably expected that their Private Information would not be shared with other unknown third parties, such as Stripe and MaxMind.

104. Shopify's actions constituted a serious invasion of privacy in that it invaded a zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and violated criminal laws on wiretapping and

invasion of privacy. These acts constitute an egregious breach of social norms that is highly offensive.

105. Shopify's intentional intrusion into the Class members' privacy was also highly offensive to a reasonable person in that Shopify violated criminal and civil laws designed to protect individual privacy and against theft. Shopify also disseminated Class members' financial and credit information.

106. Shopify lacked a legitimate business interest in enabling the Shopify Instruments to intercept, collect, transmit, receive, track, analyze, and sell the Private Information of the Class members without their consent.

107. The Class members have been damaged by Shopify's invasion of their privacy and are entitled to just compensation and injunctive relief.

Fourth Cause of Action

Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

108. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

109. A plaintiff asserting a claim for intrusion upon seclusion must plead (i) that the defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff had a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable person.

110. By enabling the Shopify Instruments to intercept, collect, transmit, receive, track, and analyze consumers' Private Information without their consent, and by communicating and/or selling that Private Information to other third parties, such as Stripe and MaxMind, Shopify intentionally intruded upon the solitude or seclusion of the Class members, in that Shopify effectively placed

itself in the middle of communications to which it was not invited, welcomed, or authorized.

111. The Class members did not consent to, authorize, or know about Shopify's intrusion at the time it occurred. Further, they never agreed that Shopify could install a tracking cookie on their devices to track them across the Shopify merchant network, nor did they agree that Shopify could transmit, receive, track, and analyze their private information, or that their private information could be disclosed to other merchants and/or other third parties such as Stripe and MaxMind.

112. Shopify's intentional intrusion on the Class members' solitude or seclusion without consent would be highly offensive to a reasonable person. The Class members reasonably expected, based on (i) the fact that they had established a secure, encrypted connection to the IABMFG website; (ii) the fact that no disclosure was made to them that Shopify was involved in the transaction that their Private Information would be submitted exclusively to the merchant, and would be used only for the purpose of making their purchase.

113. Shopify's intentional intrusion into the Class members' private conversations was highly offensive to a reasonable person in that it violated state laws designed to protect individual privacy.

114. The surreptitious taking and disclosure of personal, confidential, and private information from the Class members was highly offensive because it violated expectations of privacy that have been established by general social norms. Privacy polls and studies consistently show that the overwhelming majority of Americans believe one of the most important privacy rights is the

need for an individual's affirmative consent before personal data is harvested or shared.

115. Shopify intentionally engages in the misconduct alleged herein to generate substantial profit, not only through its transaction fees, but also by improving the functionality of its products by using consumer profiles, and by selling and/or sharing consumers' Private Information to Shopify merchants and/or other third parties, such as Stripe and MaxMind.

116. As a result of Shopify's actions, the Class members have suffered harm and injury, including but not limited to the invasion of their privacy rights.

117. Unwanted access to data by electronic or other covert means, in violation of the law or social norms is actionable under California law.

118. The Class members have been damaged as a direct and proximate result of Shopify's invasion of their privacy and are entitled to just compensation.

119. The Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by Shopify as a result of its intrusions upon the Class members' privacy.

Fifth Cause of Action

Violation of the California Computer Data Access and Fraud Act, Cal. Penal Code § 502 (On Behalf of Plaintiff and the Class)

120. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

121. Cal. Penal Code § 502 provides that any person who commits any of the following acts is guilty of a public offense:

> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

122. Smartphone devices with the capability of using mobile apps are "computers" within the meaning of the statute.

123. Shopify violated the Cal. Penal Code § 502(c)(1) and (2) by knowingly accessing Plaintiff's and the Class member's data by surreptitiously and intentionally installing software code and cookies onto their devices, including Plaintiff's iPhone. The software code and cookies enabled Shopify to take, copy, or make use of Plaintiff's and the Class members' Private Information and data from their transactions across Shopify's merchant network, as described above.

124. Shopify took, copied, or made use of Plaintiff's and the Class members' data and Private Information, even though Plaintiff and the Class members never gave Shopify permission to do so. Because Shopify intentionally designs the websites that it hosts on behalf of its merchant-customers and its payment forms to omit its involvement with the transaction, users, such as Plaintiff and the Class members, have no idea that Shopify is taking, copying or using their data. Further, Shopify failed to disclose its Privacy Policy or Terms of Use to Plaintiff and the Class members in the course of their transactions with Shopify's merchant customers and, therefore, Plaintiff and the Class members never consented to allow Shopify to take, copy or use their data. In doing so,

Shopify wrongfully obtained control of Plaintiff's and the Class members' data. That data is used to generate individualized profiles on users that Shopify markets to its merchant customers. Additionally, Shopify provides Plaintiff's and Class members' data to third parties, such as Stripe and MaxMind, among other things.

125. The Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of their right to privacy; (ii) loss of value in their Private Information; and (iii) the price premium they were unknowingly charged by IABMFG to compensate for Shopify's fees, since they would not have purchased the products had they known their data was being accessed, copied, taken, obtained and used without permission.

126. The Class members seek all relief available under Cal. Penal Code § 502(e), including compensatory damages and/or disgorgement of profits made by Shopify and injunctive or other equitable relief.

127. Plaintiff and the Class members further seek punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Shopify's conduct was willful and oppressive, fraudulent, and/or malicious as defined in Cal. Civil Code § 3294.

128. Plaintiff and the Class members also seek their reasonable attorney's fees pursuant to Cal. Penal Code § 502(e)(2).

Sixth Cause of Action

Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, et seq.
(On Behalf of Plaintiff and the Class)

129. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

130. Shopify is a "person" under Cal. Bus. & Prof. Code § 17201.

131. Shopify created and implemented a scheme to obtain the Private Information from the Class members through a pervasive pattern of false and misleading omissions. Shopify concealed and failed to disclose to the Class members the following facts: (i) that the Shopify payment forms were being provided by Shopify; (ii) that Shopify would intercept the communications, including the Private Information, that Class members reasonably believed would be sent directly and exclusively to the merchant; (iii) that Shopify would collect and store the Class members' Private Information, including information entered by them in the forms, as well as other Private Information not expressly provided by them, in its databases and/or in Stripe's databases; (iv) that Shopify would access Class members' data from their devices without authorization and install a tracking cooking on their devices and track their behavior across its entire merchant network; (v) that Shopify would sell and make that information available to its other customers and other third parties, such as Stripe and/or MaxMind, who, in turn, shared Class members' data with their own customers; (vi) that Shopify would continue to monitor the status of the transactions with their banks, including whether and why they disputed the charges; or (vii) that Shopify would use the information to affect future financial transactions performed by the Class members. Indeed, Shopify concealed and failed to disclose its identity to the Class members; it did not disclose that it was involved in the transactions at all.

132. These omissions were misleading and deceptive.

133. Shopify's conduct was unfair and unconscionable, particularly because Shopify intruded on communications that the Class members reasonably believed to be private, and also because Shopify made and/or offered to make their Private

Information available to any of its merchant customers and third parties who, at any time in the past or future, were involved in a financial transaction with the Class members. Unbeknownst to the Class members and without their consent, the third parties with whom Shopify shared Class members' data, including Stripe and MaxMind, in turn shared Class members' data with their own customers.

134. Shopify's conduct was fraudulent and deceptive because the omissions at issue were likely to, and in fact did, deceive reasonable consumers, including the Class members. Reasonable consumers, including the Class members, would have found it material to their purchasing decisions that Shopify would intercept, collect, transmit, receive, track, and analyze consumers' private information without their consent, and share that Private Information with Shopify merchants and other third parties, such as Stripe and MaxMind, who, in turn, disseminate the data to their own customers. Knowledge of these facts would have been a substantial factor in the Class members' decisions to engage in the financial transactions described herein.

135. Shopify owed the Class members a duty to disclose these facts because they were exclusively known and/or accessible to Shopify, who had superior knowledge of its activities with respect to the private information of the Class members; because Shopify actively concealed the facts; and because Shopify intended for consumers to rely on the omissions in question.

136. As set forth above, in engaging in financial transactions using Shopify payment forms, the Class members relied on Shopify's omissions. Reasonable consumers would have been expected to have relied on the omissions, particularly because they had directed their browsers and/or mobile applications to visit and establish secure connections to the merchant's website, and because they were not

informed that Shopify would intercept and receive their communications, which they believed would be sent directly and exclusively to the merchant over the secure connection with the merchant website.

137. Shopify has engaged, and continues to engage, in unlawful practices as described herein, in violation of the Unfair Competition Law, California Business & Professions Code §§ 17200 *et seq.* (the "UCL"), by, without limitation, violating the following statutes: the California Invasion of Privacy Act, Cal. Penal Code §§ 635 and 637; the California Online Privacy Protection Act of 2003 ("CalOPPA"), Cal. Bus. & Prof. Code § 22575 *et seq*.; the California Consumer Privacy Act of 2018 ("CCPA"), Cal. Bus. & Prof. Code § 1427 *et seq*; and the California Computer Data Access and Fraud Act, Cal. Penal Code § 502. Shopify's conduct was also unlawful because it intruded upon Plaintiff's and the Class members' seclusion and violated the California Constitution by invading Class members' privacy, as described above.

138. Shopify was subject to CalOPPA because it is an entity that owns or operates a commercial website or online service that collects and maintains personally identifiable information, including California consumers' first and last names, street address, email address, telephone number, who use or visit said website or online service. Shopify violated CalOPPA because it does not conspicuously post its privacy policy on websites it operates on behalf of its merchant customers or websites in which Shopify performs online services. These websites fail to include Shopify's privacy policy or a text or icon link to Shopify's privacy policy on the merchant customers' homepages or first significant page after entering the website.

139. Shopify also violated the CCPA because, among other things, it is a business that controls the collection of consumers' personal information and fails to make any of the disclosures required pursuant to Cal. Bus. & Prof. Code § 1798.100 at or before it collects consumers' personal information.

140. Shopify engaged in conduct that is unfair and unconscionable because its activities with respect to Class members' Private Information offends public policy, is immoral unethical, oppressive, outrageous, unscrupulous, and substantially injurious, and has caused substantial harm that greatly outweighs any possible utility from the conduct.

141. Shopify's conduct actually and proximately caused the Class members to lose money or property. Absent Shopify's unlawful, unfair, and fraudulent conduct, Plaintiff and Class Members would have behaved differently and would not have entered into financial transactions with merchants such as IABMFG. Further, Shopify's unlawful activities and use of the Class members' Private Information enabled it to charge transaction fees to merchants, the price of which the Class members covered through increased merchant fees.

142. Plaintiff seeks, on behalf of himself and those similarly situated, equitable relief, including restitution for the premium and/or the full price that he and others paid as result of Defendants' conduct. Plaintiff and the Class lack an adequate remedy at law to obtain such relief with respect to their "unfairness" claims in this UCL cause of action, because there is no cause of action at law for "unfair" conduct. Plaintiff and the Class similarly lack an adequate remedy at law to obtain such relief with respect to their "unlawfulness" claims in this UCL cause of action because CalOPPA and CPPA do not provide a direct cause of action, so

Plaintiff and the Class must allege those violations as predicate acts under the UCL to obtain relief.

143. Plaintiff also seeks equitable relief, including restitution, with respect to their UCL unlawfulness claims for violations of the CLRA, FAL and her UCL "fraudulent" claims. Pursuant to Federal Rule of Civil Procedure 8(e)(2), Plaintiff makes the following allegations in this paragraph as an alternative to any contrary allegations in their other causes of action, in the event that such causes of action do not succeed. Plaintiff and the Class may be unable to obtain monetary, declaratory and/or injunctive relief directly under other causes of action and will lack an adequate remedy of law. For example, Plaintiff and the Class may be unable to obtain such relief under other causes of action and will lack an adequate remedy at law, if Plaintiffs are unable to demonstrate the requisite *mens rea* (intent, reckless, and/or negligence), because the UCL imposes no such *mens rea* requirement and liability exists even if Defendants acted in good faith.

144. Plaintiff seeks, on behalf of himself and those similarly situated, a declaration that the above-described trade practices are fraudulent, unfair, and/or unlawful.

145. Plaintiff seeks, on behalf of himself and those similarly situated, an injunction to prohibit Defendants from continuing to engage in the deceptive and/or unlawful trade practices complained of herein. Such misconduct by Defendants, unless and until enjoined and restrained by order of this Court, will continue to cause injury in fact to the general public and the loss of money and property in that Shopify will continue to violate the laws of California, unless specifically ordered to comply with the same. This expectation of future violations will require current and future consumers to repeatedly and

continuously seek legal redress in order to recover monies paid to Shopify to which they were not entitled. Plaintiffs, those similarly situated and/or other consumers nationwide have no other adequate remedy at law to ensure future compliance with the California Business and Professions Code alleged to have been violated herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and those similarly situated, respectfully requests that the Court enter judgment against Defendants as follows:

A. Certification of the proposed Class, including appointment of Plaintiff's counsel as class counsel;

B. An award of compensatory damages, including statutory damages where available, to Plaintiff and the Class Members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including both pre- and post-judgment interest thereon, except as to those causes of action where compensatory damages are not legally available;

C. An order for full restitution;

D. An order requiring Defendants to disgorge revenues and profits wrongfully obtained;

E. An order temporarily and permanently enjoining Defendants from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

F. For reasonable attorneys' fees and the costs of suit incurred; and

G. For such further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: January 24, 2022

GUTRIDE SAFIER LLP

/s Seth A. Safier

Seth A. Safier, Esq.
Marie A. McCrary, Esq.
Todd Kennedy, Esq.
Hayley Reynolds, Esq.
100 Pine Street, Suite 1250
San Francisco, CA 94111

Kali Backer, Esq. (*pro hac vice*)
4450 Arapahoe Ave.
Suite 100
Boulder, Colorado 80303